CRYPTOME

Donate for the Cryptome archive of files from June 1996 to the present

---

10 November 2014

Lawrence Baldwin Darknet Spy

---

http://dealbook.nytimes.com/2014/11/09/on-the-hunt-for-hackers-but-not-the-spotlight/

On the Hunt for Wall St. Hackers, but Not the Spotlight

By Nicole Perlroth and Matthew Goldstein

November 9, 2014

Lawrence Baldwin, left, at Defcon, a convention of computer hackers, in Las Vegas in 2002.
YouTube

Lawrence Baldwin is a dark hero of the Internet whom you have probably never heard of — and for good reason.

A decade ago, Mr. Baldwin made a name for himself and his Atlanta-based security firm, myNetWatchman, by collecting and analyzing digital scourges like malware, and alerting companies to them. He was a fixture on the security conference circuit and was often quoted in the press about security threats.

And then he seemed to disappear. Beyond a bare-bones website and a LinkedIn profile where his only listed interest is “chasing down cybercriminals and smacking them upside the head,” Mr. Baldwin largely vanished from the web.

“If you look for me on Google, you’d be hard pressed to find my involvement in anything for the last seven or eight years,” he said.

Yet Mr. Baldwin is well known to a number of large United States banks and financial institutions that have turned to him for help in combating increasingly sophisticated hacking attacks.

He declined to discuss his work for the banks, citing concerns about his personal safety.

For the past seven years, several security consultants and former law enforcement personnel say, Mr. Baldwin has immersed himself in the so-called dark web, using what most describe as unorthodox methods to gather intelligence about online financial crime. Mr. Baldwin, 49, says that he is able to closely monitor many of the criminals who he says have made "hundreds of millions of dollars" hacking into American banks and corporations.

It is that unusual proximity — and the reliable information that it produces — that has made Mr. Baldwin one of the go-to consultants for financial institutions. Those familiar with his work say he is one of the consultants used by banks like JPMorgan Chase, which is still dealing with the fallout from an intrusion that compromised some information for 76 million households and seven million small businesses.

To his supporters, Mr. Baldwin, who has a degree in computer science from the University of Hartford, is something of a secret agent. "He has eyes directly on the perpetrator," said one security expert who did not want to be identified because of Mr. Baldwin's preference for a low profile.

Another described his work as "very cloak and dagger." All agree that the intelligence he provides is very effective. "I would take his intelligence over anyone else's any day of the week," another said.

Companies often complain that when they are breached, they rarely learn anything about their attackers from law enforcement. Security companies are also little help. Many victims of breaches say these companies bury their analysts in heaps of data without offering any context or attribution. By the time chief information security officers discover that their data has left the building, executives complain, the criminals have already moved on.

All of this has created a market for a handful of consultants like Mr. Baldwin who go undercover and track the criminals' activity in real time.

"Baldwin stands out because he provides actionable intelligence," said Avivah Litan, a security analyst with Gartner, the research firm. "It's exact, it's original and he barely charges for it, whereas other firms repackage intelligence from many sources."

She added, "There's a finite number of original sources for intelligence on bad activities."

Yet while banks and Wall Street firms rely on Mr. Baldwin's services, they do not like to talk about it.

A spokeswoman for JPMorgan said she could not comment on whether the bank consulted with Mr. Baldwin. JPMorgan, which spends $250 million annually on digital security, has about 1,000 dedicated security personnel. But the bank also works with a handful of outside-threat intelligence providers in addition to consulting firms like Booz Allen Hamilton and Stroz Friedberg to investigate attacks, said other people briefed on the matter.

For his part, Mr. Baldwin maintains that he did not work directly with JPMorgan to solve its recent breach.

He was slightly more open in March about his work, as he discussed the details of a recent attack against a bank during a presentation to the Georgia Banking Association. Mr. Baldwin asked the attendees not to discuss the talk with reporters.

The reason for the banks' caution is that the information Mr. Baldwin provides becomes useless as soon as it is made public — and because many of his clients are not quite sure where Mr. Baldwin's information comes from.

Two people familiar with his methods said that Mr. Baldwin's company maintains listening posts on Internet service provider networks and infects tools used by criminals, like underground botnets — networks of infected computers — to see what criminals are collecting and where they are collecting it from. He has also developed a web of contacts across industries and knows who is stealing information.

"He has gone underground and become privy to what they're developing," said Ms. Litan, of Gartner. "There's no other way. It's the way."

A few years ago, law enforcement officials spoke to Mr. Baldwin to ensure he understood what he could do without breaking the law, according to two people briefed on the conversation. One concern is that while Mr. Baldwin has a record of developing intelligence on hacker activity, the information cannot be used as evidence in a criminal proceeding because of his methods, and the confidential relationships he uses to gather it.

Still, law enforcement officials who have worked with him describe Mr. Baldwin as a valuable partner.

Thomas Grasso, a supervisory special agent with the F.B.I., said the bureau "had a very good working relationship with Mr. Baldwin and his company over the years," and had worked with him and others in the private sector to stay ahead of online threats.

Mr. Baldwin did not start out as a security guru. Early in his career he worked at BellSouth, helping to introduce its dial-up network. Immediately, hackers tried to break in. What began as a curiosity — figuring out who they were and how they attacked their victims — became his life's work.

In an industry dominated by those who charge high fees for other people's intelligence, one person said, Mr. Baldwin stands out as a "boy scout" who simply wants to catch criminals and routinely shares information free. With prosecutions and extraditions of hackers rare, Mr.

Baldwin is motivated, say those familiar with him, to do everything possible to disrupt their businesses.

He works closely with the National Cyber-Forensics and Training Alliance, a nonprofit based in Pittsburgh that brings together law enforcement, private industry members, security consultants and academic scholars to share information to prevent and mitigate the threats. The group works closely with many American banks and corporations and has received contributions in recent years from Bank of America, Microsoft and Symantec.

Some have likened Mr. Baldwin's sleuthing to that of Brian Krebs, the security blogger who earned attention investigating Russian spammers and has been pranked by spammers as a result. But security researchers say Mr. Baldwin's investigations take him much deeper into the netherworld of the web.

That explains Mr. Baldwin's low profile over the past few years. "I'm not a press hound," he said. "There are serious personal safety issues to consider."
